宏洲纖維工業股份有限公司・資安風險評估分析（112）

紡織產業歷經多年來從各種危機中轉型蛻變，不斷的提升經營、生產之管理能力，為產品開發差異性、注入活水，市場的型態也逐漸由以量制價，轉型為以功能性、高附加價值的競爭，值此工業 4.0、AI 人工智慧、雲端化等各類先進技術融合的數位轉型時代，本公司所處化纖產業，以往所高度依賴之生產設備及人力，亦面臨優存劣汰之十字路口，結合科技的整合效益將厚實企業未來的競爭力及拓展商機；相對在大量資訊技術的引進下，資訊環境的穩定度及安全性，將決定企業追求創新、品質、快速地提供產品或服務的關鍵，是營運上不可忽略的一環。

本公司對資訊環境維護及生產設備功能提升方面之投資，均秉持適用、適時、適量之原則，對資安風險之控管亦遵照內部控制制度，及參考外部實例或廠商建議而持續改進；針對資安風險之評估，乃依下列 10 個類別 209 個查核項目(依 ISACA 國際電腦稽核協會台灣分會之"資通安全公司自我檢查表"加以修訂)，定期於每年 12 月至隔年 1 月間進行自我評估及分析，依查核項目之達成度或完整性給予高、中、低評比並予量化統計後，再依據風險性較高的部份進行檢討及擬具改善措施，近期執行的時間為 2022 年 10 月 17~19 日，由資訊人員執行，報告呈總經理核閱，並提供內、外部稽查。

由於本公司的生產設備均為獨立運作，並未透過資訊系統(例如: MES 製造執行系統)及網路做資料集結和進一步之運用，且資訊管理系統僅限於公司區域網路執行，未開放透過網際網路之連線，自評中在機敏性資料的防護處理上較為不足，提高風險度，改善措施將汰換舊版電腦為 Windows 10，並擬請資安廠商進行外部偵測及稽核等相關服務，以加強資安防護之強度及增加風險評估之可信度，總結整體之資安風險程度介於"低-中"之間，無重大營運風險。

項次	評估類別	風險評比(%)			重要管控措施
		低	中	高	
1	資訊安全政策	70	30	0	1.定期審查、修訂資訊安全政策。 2.內部稽核單位每年定期稽查管控措施。
2	建立資訊安全組織	64	36	0	1.設資安管理小組及個人資料保護小組。 2.訂立資安事件之緊急應變處理及回報程序。
3	人員安全與管理	30	70	0	1.內部控制制度定義資訊人員、使用者之作業權限畫分，及人員異動、離職之作業準則。 2.每年執行作業權限複核。 3.每年定期普查個人電腦，防止公器私用。
4	資產分類與控管	33	67	0	1.資訊類軟、硬體資產列冊管理。 2.每年定期普查電腦，確認軟、硬體資產。
5	實體及環境安全管理	79	21	0	1.專用電腦機房具溫度、電力自動控管。 2.伺服器及重要職務之電腦，安裝防毒軟體，每日

					定時備份，其備份份數至少二代。 3.營運資料庫資料每日壓縮後以磁帶儲存備份，每年定期模擬事故演練於廠商備援機房還原測試。
6	通訊與操作管理	64	36	0	1.電子郵件主機具自我防護及保存稽核之功能。 2.每日分析防火牆紀錄，並使用上網行為記錄器，即時防堵內、外部異常行為。 3.即時宣導資安事件、通告或案例，提升防護意識。 4.使用 Hinet 資安艦隊之防護方案，擴展防護廣度。
7	存取控制	71	29	0	1.電子檔資料依部門、個人設定存取權限。 2.對外連線作業申請需經部門主管及總經理同意。 3.電子郵件區分內、外部，不須對外連絡之人員僅能內部寄信。 4.人力資源系統於讀取個資時，自動記錄存取軌跡。
8	系統開發與維護	76	24	0	應用系統自行開發、維護，在規劃分析時主動將安全需求納入設計考量，防範外部的侵入篡改。
9	永續運作之計畫管理	60	40	0	1.營運資料庫每年定期演練、測試。 2.重要設備訂立緊急應變計劃，供發生重大資安事件時遵循及應變。
10	內部稽查及其它	55	45	0	1.每年電腦普查時告知公司軟體所授權之範圍，實際查核若有規範以外軟體則要求移除或提供授權證明；軟、硬體普查資料，隨時依資產狀況更新。 2.資訊單位每年定期自評資訊作業環境安全。 3.內部稽核人員每年定期稽查資訊控制作業。
總　　評（%）		65	35	0	1.舊版 Windows 個人電腦應汰換。 2.應加強機敏性資料的防護措施。